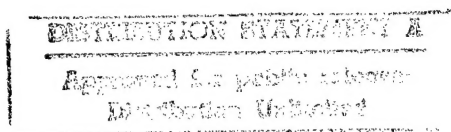


September 1997

DEPARTMENT OF ENERGY

DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories



19971118 018

DLIC QUALITY INSPECTED 3



United States
General Accounting Office
Washington, D.C. 20548

**Resources, Community, and
Economic Development Division**

B-277671

September 25, 1997

The Honorable Floyd D. Spence
Chairman
The Honorable Ronald V. Dellums
Ranking Minority Member
Committee on National Security
House of Representatives

As directed by the Committee in House Report No. 104-563, this report addresses the Department of Energy's (DOE) controls over foreign visitors to its three nuclear weapons laboratories. Specifically, the report discusses DOE's (1) procedures for reviewing the backgrounds of foreign visitors and for controlling the dissemination of sensitive information to such visitors, (2) security controls for limiting foreign visitors' access to areas and information within its laboratories, and (3) counterintelligence programs for mitigating the potential threat posed by foreign visitors.

As arranged, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will provide copies of the report to the Secretary of Energy; the Director, Office of Management and Budget; and other interested parties. We will also make copies available to others upon request.

Please call me on (202) 512-3841 if you or your staffs have any questions. Major contributors to this report are listed in appendix V.

A handwritten signature in black ink, appearing to read "Victor S. Rezendes".

Victor S. Rezendes
Director, Energy, Resources,
and Science Issues

Executive Summary

Purpose

With the end of the Cold War, the Department of Energy's (DOE) weapons laboratories are moving away from secret nuclear weapons research toward unclassified cooperative research involving a variety of nations and an increasing number of foreign visitors. This openness greatly benefits DOE and the United States by stimulating the exchange of ideas, promoting cooperation, and enhancing research efforts. However, while foreign visitors are providing benefits to DOE's programs, the weapons laboratories are key targets of foreign intelligence interest, according to counterintelligence experts, thus raising concerns about possible espionage efforts against those laboratories, including industrial espionage.

To guard against foreign nationals' obtaining information that would be detrimental to U.S. security or business interests, DOE has established various controls to minimize the risk of foreign espionage. However, past work done by GAO in 1988 and more recently by elements of the U.S. intelligence community has shown problems with DOE's controls over foreign visitors to its laboratories.¹ Moreover, because the number of foreign visitors to the laboratories increased over 50 percent from the late-1980s to the mid-1990s, additional burdens have been placed on the controls DOE has in place to manage foreign visits. The high number of foreign visitors, as well as some recent investigative cases involving foreign nationals at DOE's laboratories, have increased concerns that the laboratories are targets of foreign espionage.

Because of these concerns, the House Committee on National Security, in a May 1996 report, directed GAO to determine how well DOE has been managing foreign visits to the weapons laboratories. Accordingly, GAO assessed DOE's (1) procedures for reviewing the backgrounds of foreign visitors and for controlling the dissemination of sensitive information to them, (2) security controls for limiting foreign visitors' access to areas and information within its laboratories, and (3) counterintelligence programs for mitigating the potential threat posed by foreign visitors.

Background

Historically, the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, and the Sandia National Laboratories have been responsible for conducting research and development for DOE's nuclear weapons program. The laboratories are also world-leading centers of research in many technologies and scientific disciplines and conduct a

¹Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31, Oct. 11, 1988).

broad range of nonnuclear research activities in such areas as biomedicine, high-performance computers, and environmental restoration. DOE's policy encourages international cooperation in unclassified energy and science programs to obtain the benefits of scientific and technical advances from other countries and to minimize research costs. Consequently, each year thousands of foreign nationals visit these three laboratories to participate in cooperative research or laboratory programs.

DOE Order 1240.2b establishes controls over unclassified foreign visits (stays of up to 30 days) and assignments (extended stays of up to 2 years).² Among other things, this order requires that DOE obtain background information on certain proposed visitors from sensitive countries—countries considered to be a risk to security or nuclear proliferation. The order also requires that DOE review and approve visits involving information that, although unclassified, is considered sensitive for such reasons as its potential to enhance nuclear weapons capability, lead to nuclear proliferation, reveal advance technologies, or have “dual-use” applications (technologies that have both peaceful and military uses). In addition, each weapons laboratory has security procedures for controlling foreign nationals' access to its facilities. Furthermore, DOE has established counterintelligence programs at headquarters and the laboratories to mitigate the risk of foreign espionage, increase employee awareness, and brief and debrief employees serving as hosts to foreign visitors. Counterintelligence programs have become more important as the number of foreign visitors has increased.

Results in Brief

DOE's procedures for obtaining background checks and controlling the dissemination of sensitive information are not fully effective. DOE has procedures that require obtaining background checks, but these procedures are not being enforced. At two of the laboratories, background checks are conducted on only about 5 percent of the foreign visitors from countries that DOE views as sensitive. GAO's review of available data from DOE and the Federal Bureau of Investigation showed that some of the individuals without background checks had suspected foreign intelligence connections. Furthermore, DOE's procedures lack clear criteria for identifying visits that involve sensitive subjects and process controls to help ensure that these visits are identified. As a result, sensitive subjects may have been discussed with foreign nationals without DOE's knowledge and approval.

²For purposes of this report, we use “visit” as a generic term for both short-term visits or long-term assignments. However, we do make distinctions between visits (or visitors) and assignments (or assignees) in situations where such distinctions are significant.

DOE's security controls, such as access restrictions, in the areas most visited by foreign nationals do not preclude their obtaining access to sensitive information, and problems with the control of this information—such as sensitive information being left in an open hallway accessible to foreign visitors—have occurred at the laboratories. Furthermore, DOE has not evaluated the effectiveness of the security controls over this information in those areas most frequented by foreign visitors.

The DOE headquarters and laboratory counterintelligence programs are key activities for identifying and mitigating foreign intelligence efforts, but these programs have lacked comprehensive threat assessments, which identify likely facilities, technologies, and programs targeted by foreign intelligence. Such assessments are needed as a critical component of a more sophisticated security strategy that is consistent with the laboratories' more open missions. Furthermore, DOE could use these assessments to develop the performance measures needed to guide the laboratories' counterintelligence programs and to gauge their effectiveness. Currently, DOE has not developed such performance measures or evaluated the effectiveness of its counterintelligence programs.

Principal Findings

Procedures Are Not Effectively Implemented

DOE Order 1240.2b requires the laboratories to submit information to DOE for background checks for all foreign visitors from sensitive countries and to obtain these checks in advance for those who are on assignment at the laboratories. Consistent with these requirements, Livermore obtained background checks on 44 percent of its visitors from sensitive countries. However, to reduce costs and processing backlogs, the Los Alamos and Sandia laboratories implemented in 1994 a partial exception that DOE had granted to the order that largely avoided the background check process. Since then, DOE has obtained background checks on about 5 percent of the visitors from sensitive countries to these two laboratories. GAO's review of available data from DOE and the Federal Bureau of Investigation showed that, as a result of obtaining fewer background checks for foreign visitors to these laboratories, questionable visitors, including suspected foreign intelligence agents, had access to the laboratories without DOE and/or laboratory officials' advance knowledge of the visitors' backgrounds.

DOE's existing procedures for identifying sensitive subjects lack clear criteria for determining which subjects are sensitive and process controls to help ensure that proposed visits involving potentially sensitive subjects are reviewed by officials at DOE headquarters. Consequently, although the laboratories identified 72 visits involving sensitive subjects during the 1994 to 1996 timeframe, GAO identified other visits that occurred without DOE's review and approval and that may have involved sensitive subjects, such as inertial confinement fusion (a technology with both energy and nuclear weapons applications) and the detection of nuclear weapons testing. Although DOE and laboratory officials have recognized problems with identifying sensitive subjects and are taking actions to better identify them, their actions are not yet completed.

Security Controls Leave Vulnerabilities

The controls in the areas of the laboratories that are most often visited by foreign nationals do not preclude their access to sensitive information. Foreign visitors are generally allowed into "property protection," or controlled areas. These areas have lower levels of controls than do security areas in which classified work is conducted. For example, in contrast to the controls in place in security areas, foreign visitors are, in some cases, allowed unescorted, 24-hour access to facilities in controlled areas. Security problems and vulnerabilities involving foreign visitors and sensitive—and in some cases even classified—information have occurred or been identified by the laboratories. For example, at one laboratory, several boxes marked "sensitive materials" were left in a hallway accessible to foreign visitors. At another laboratory, classified information was included in a newsletter sent to 11 foreign nationals.

Thorough assessments and surveys of the controls over foreign visitors' access to sensitive information have not been conducted. Although some security assessments of limited scope done by the laboratories have demonstrated the vulnerability of sensitive information to being compromised, these assessments have generally examined specific buildings or programs and have not focused on controls over sensitive information in the areas most accessed by foreign visitors. Likewise, DOE's broader security surveys of its weapons laboratories have not assessed the effectiveness of the controls over sensitive information, either in general or in relation to foreign visitors.

Counterintelligence Programs Could Be Improved

DOE's counterintelligence programs have not been based on a comprehensive threat assessment that examines the nature and extent of foreign espionage activities. Such an assessment would analyze the

countries of concern and identify for the entire Department the technologies, information, and programs likely to be targeted by these countries. Counterintelligence officials at both DOE and the Federal Bureau of Investigation believe this assessment is needed as a basis for guiding DOE's counterintelligence programs and ensuring that their efforts are properly focused; however, DOE has not conducted such an assessment because of programmatic priorities and the lack of sufficient analytical expertise. Furthermore, DOE has not provided detailed oversight of the laboratories' counterintelligence programs. In this regard, DOE has not developed expectations and performance measures for those programs or periodically evaluated them.

DOE is now taking steps to improve its counterintelligence programs. The Congress provided DOE with an additional \$5 million in fiscal year 1997 to expand counterintelligence activities; DOE is using about half of these funds for the counterintelligence programs at the three nuclear weapons laboratories. Also, DOE and the laboratories are undertaking various initiatives to improve their counterintelligence efforts, such as developing more thorough threat assessments. Although implementation of these improvements is scheduled for the end of fiscal year 1997, DOE counterintelligence officials raised concerns that the Department may not fully implement these improvements in light of its historical lack of support for its counterintelligence program.

Recommendations

GAO is making several recommendations to the Secretary of Energy that are designed to (1) obtain background checks on more of the foreign visitors to the Department's weapons laboratories, (2) improve the identification and review of visits by foreign nationals that involve sensitive subjects, (3) more thoroughly assess the adequacy of security procedures in unclassified areas of the weapons laboratories, and (4) enhance the effectiveness of counterintelligence programs at DOE's headquarters and laboratories.

Agency Comments

GAO provided a draft of this report to DOE for its review and comment. In its written response, DOE had no comments on the general nature of the facts presented in the draft report and concurred with all the recommendations. DOE believes, however, that the report overstates the value of background checks on foreign visitors. GAO recognizes that background checks are but one factor to be considered in approving foreign visits and recommends only that DOE obtain background checks in accordance with its foreign

visit and assignment order. DOE also suggested that GAO revise the language for one recommendation regarding an assessment of security procedures at each laboratory. Although DOE suggested that GAO specify that a certain type of assessment be conducted, GAO did not revise the recommendation in order to avoid being overly prescriptive in how such assessments are performed. Finally, as DOE suggested, GAO clarified the recommendation to focus more clearly on protecting sensitive information.

DOE's response also detailed a number of initiatives it has taken or plans to undertake that address the recommendations. DOE's comments and GAO's evaluation are included at the end of chapter 5; the full text of DOE's comments are included as appendix IV.

Contents

Executive Summary		2
<hr/>		
Chapter 1		10
Introduction	DOE's Weapons Laboratories	10
	Controls Over Foreign Visits to the Weapons Laboratories	16
	Concerns Exist About the Potential Compromise of Sensitive Information	19
	Objectives, Scope, and Methodology	21
<hr/>		
Chapter 2		24
Foreign Visitor	DOE Has Little Advance Knowledge About the Backgrounds of Many Visitors From Sensitive Countries	24
Procedures Have Not Been Effectively Implemented	DOE Has Not Adequately Ensured That Visits Involving Sensitive Subjects Are Identified and Reviewed	28
<hr/>		
Chapter 3		33
Security Controls May Not Adequately Protect Sensitive Information From Foreign Visitors	Security Requirements in Controlled Areas	33
	Security Vulnerabilities and Problems Have Involved Foreign Visitors	36
	Protection of Sensitive Information in Controlled Areas Has Not Been Fully Assessed	37
<hr/>		
Chapter 4		40
DOE's Counterintelligence Efforts Can Be Improved	DOE's Headquarters and Laboratory Counterintelligence Programs	40
	DOE Has Not Clearly Defined the Threat Posed by Foreign Visitors to Its Laboratories	42
	DOE Has Not Effectively Overseen the Laboratories' Counterintelligence Programs	43
	DOE Is Taking Steps to Strengthen Its Counterintelligence Program	45
<hr/>		
Chapter 5		47
Conclusions and Recommendations	Recommendations	48
	DOE's Comments and Our Response	49

Appendixes

Appendix I: DOE's List of Sensitive Countries	52
Appendix II: DOE's List of Sensitive Subjects	53
Appendix III: Number and Percentage of Background Checks Obtained for Foreign Visitors From Sensitive Countries to DOE's Nuclear Weapons Laboratories, 1994-96	55
Appendix IV: Comments From the Department of Energy	56
Appendix V: Major Contributors to This Report	63

Table

Table 2.1: Background Checks That Were Obtained on Sensitive-Country Visitors to DOE Weapons Laboratories, 1994-1996	26
--	----

Figures

Figure 1.1: Lawrence Livermore National Laboratory	11
Figure 1.2: Los Alamos National Laboratory	13
Figure 1.3: Sandia National Laboratories	15
Figure 1.4: Unclassified Foreign Visits to DOE's Weapons Laboratories, 1994-96	17

Abbreviations

CIA	Central Intelligence Agency
DOE	Department of Energy
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
OPSEC	operations security

Introduction

Although the Cold War has ended, the threat of foreign espionage to the nation still exists from a variety of countries, and recent revelations of intelligence activities against the United States involving Russia, China, and South Korea have raised concerns that such activities are on the increase. The Department of Energy (DOE) and its facilities, especially its nuclear weapons laboratories, are key targets of foreign intelligence interest. Not only do these laboratories conduct activities related to the design, construction, and maintenance of nuclear weapons—a long-standing target of foreign espionage—but they also conduct research into many areas of high technology, such as laser fusion, high-performance computers, and microelectronics. Their research is often done in collaboration with industry, and sometimes foreign countries, to develop new technologies for commercial applications. Accordingly, their work is of interest to other countries, and thousands of foreign nationals visit these laboratories each year to participate in such research. The high number of foreign visitors, as well as some recent investigative cases involving foreign nationals at DOE's laboratories, have increased concerns that these laboratories are targets of foreign espionage efforts.

DOE's Weapons Laboratories

DOE's nuclear weapons laboratories—the Lawrence Livermore National Laboratory in California and the Los Alamos National Laboratory and Sandia National Laboratories in New Mexico—have been the cornerstones of the U.S. weapons program for over 40 years. In this regard, they are unique among DOE's laboratories.¹ Government-owned and contractor-operated, these three laboratories have been assigned specific missions for nuclear weapons development as well as other programmatic responsibilities. Over time, the laboratories have increasingly expanded their responsibilities in nondefense research areas.

The Lawrence Livermore National Laboratory is operated by the University of California for DOE. Established in 1952, the laboratory occupies 1-square mile in Livermore, California. The laboratory's major missions include nuclear weapons research and development to ensure the safety, security, and reliability of the U.S. nuclear weapons stockpile; other weapons and defense-related activities for DOE and the Department of Defense; inertial confinement fusion (a technology that has both energy and nuclear weapons testing applications); and nuclear nonproliferation.

¹DOE has 9 multiprogram and approximately 21 specialized laboratories.

Figure 1.1: Lawrence Livermore National Laboratory



Source: Lawrence Livermore National Laboratory.

The Los Alamos National Laboratory, also operated by the University of California for DOE, was established in 1943 as part of the Manhattan Project that developed the first nuclear weapons. Located approximately 35 miles from Santa Fe, New Mexico, the laboratory covers an area of

approximately 43 square miles. The laboratory conducts an array of classified and unclassified activities, including all phases of nuclear weapons research, design, and testing; other weapons-related research for DOE; and management of special nuclear materials, such as plutonium. Recently, Los Alamos was given responsibility for the production of certain weapons components.

Figure 1.2: Los Alamos National Laboratory



Source: DOE.

The Sandia National Laboratories are operated for DOE by the Lockheed Martin Corporation. Sandia, established in 1949, is located in Albuquerque, New Mexico, and works in conjunction with Livermore and Los Alamos to design and develop nuclear weapons.² Sandia conducts research, development, and engineering on all facets of weapons design and development except the nuclear explosive components. Sandia also produces some of the nonnuclear components, such as neutron generators, that are needed for nuclear weapons.

²Sandia also has a facility located adjacent to the Livermore laboratory in California.

Figure 1.3: Sandia National Laboratories



Source: DOE.

Although the Livermore, Los Alamos, and Sandia laboratories are involved in research and development activities related to nuclear weapons, in recent years many of their efforts have expanded beyond issues strictly related to defense or national security. The laboratories are now involved in such areas as high-performance computers, lasers, and microelectronics. Furthermore, they perform research in such diverse

areas as biomedicine, environmental restoration, and global climate change. In addition, the laboratories are working with industry to develop new technologies and products for the commercial market. Such activities include work on advanced automobile propulsion systems, medical applications, and waste management. Furthermore, each laboratory conducts basic scientific research in areas of its own choosing—termed Laboratory Directed Research and Development. This research involves such subjects as astrophysics and space science, particle physics, materials science, and chemistry.

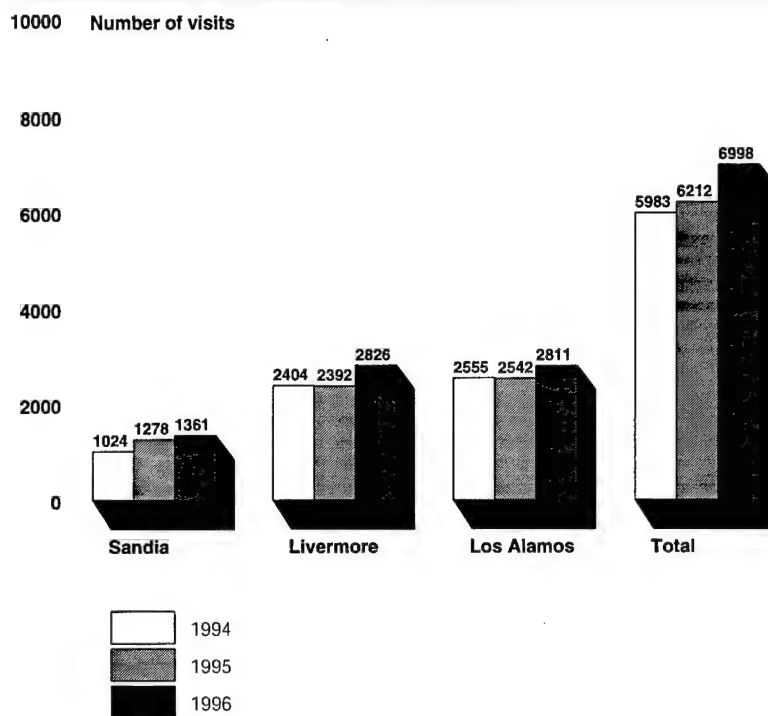
Controls Over Foreign Visits to the Weapons Laboratories

Because the Livermore, Los Alamos, and Sandia laboratories are world-leading centers of research in many technologies and scientific disciplines, many foreign scientists are attracted to them and invited to come there to exchange information or participate in research activities. DOE's policy supports an active program of unclassified visits to these laboratories for the benefit of its programs.³ In fact, DOE and the laboratories have cooperative activities with certain countries to exchange scientists and information and to collaborate on research in selected scientific areas.

With the easing of global tensions since the breakup of the Soviet Union and the changing missions of the weapons laboratories, the number of unclassified foreign visits to the laboratories has increased significantly. The average annual number of visits by foreign nationals to the laboratories has increased over 50 percent from the late-1980s to the mid-1990s. Furthermore, this increase in foreign visitors is continuing. As shown in figure 1.4, the number of unclassified foreign visits to the laboratories has increased each of the last 3 years, to a level of about 7,000 visits in 1996. This represents a significant portion of the 20,000 or more unclassified foreign visits estimated by DOE to have occurred at all of its laboratories during 1996.

³DOE allows classified foreign visits that relate to information on nuclear weapons; however, according to DOE, visits involving classified information are limited mainly to foreign nationals from the United Kingdom and countries in the North Atlantic Treaty Organization.

Figure 1.4: Unclassified Foreign Visits to DOE's Weapons Laboratories, 1994-96



Source: GAO's analysis of data from DOE and its laboratories.

Allowing foreign nationals to visit the weapons laboratories and participate in their unclassified activities provides valuable benefits to the laboratories and the country, such as using the visitors' skills to increase the chances of making significant scientific advancements. However, because such visits are not without risk, DOE Order 1240.2b—Unclassified Visits and Assignments by Foreign Nationals, September 3, 1992—establishes responsibilities and policies and prescribes administrative procedures for controlling unclassified visits and assignments to DOE's facilities. Until recently, the foreign visitor program was principally administered by the Office of Policy and International Affairs, but in March 1997 this responsibility was transferred to the Office of Resource Management in the Office of Nonproliferation and National Security. Other principal organizations involved in administering and controlling unclassified foreign visits include the Nuclear Transfer and Supplier Policy Division, Office of Arms Control and Nonproliferation; the

Office of Safeguards and Security, Office of Security Affairs; the Counterintelligence Division, Office of Energy Intelligence; the appropriate headquarters program office that is sponsoring the visit; DOE field offices; and laboratory management.

As defined by the order, visits are short-term stays of 30 days or less for the purposes of orientation, technical discussions, observation of projects or experiments, training, or discussion of collaboration on topics of mutual interest. Assignments are long-term stays of more than 30 days (within a 12-month period) to actively participate in the work of a facility or contribute to its projects. Assignments are limited to 2 years but may be extended. Assignees may include foreign nationals who are employees, as well as those who are guests or consultants.⁴ According to DOE's estimates, over 25 percent of the foreign visitors to its weapons laboratories are assignees.

DOE's foreign visit and assignment order identifies several requirements for reviewing, approving, and documenting foreign nationals' access to its nuclear weapons laboratories. Although the order, in general, allows most foreign nationals access with little oversight by DOE, the Department views some visits and assignments to be of potential concern. These include visits from countries DOE considers sensitive for reasons of national security, nuclear nonproliferation, regional instability, or terrorism support (see app. I for a list of these countries). Data from DOE and the laboratories show that almost 30 percent of the visitors to its weapons laboratories are from sensitive countries. DOE is also concerned about visits involving subjects which, although unclassified, are considered sensitive because they have the potential to enhance nuclear weapons capability, lead to nuclear proliferation, divulge militarily critical technologies, or reveal other advanced technologies (see app. II for a list of these subjects) as well as visits to areas located within the laboratories where special nuclear material and/or classified information and equipment are located.

Certain requirements must be met if a foreign visit or assignment involves a sensitive country, a sensitive subject, or a security facility where classified work is conducted. According to the foreign visits and assignments order, all assignments and visits involving sensitive subjects or security facilities where classified work is conducted must be reviewed and approved by DOE. Furthermore, before an assignment involving a

⁴For purposes of this report, we use "visit" as a generic term for both short-term visits or long-term assignments. However, we do make distinctions between visits (or visitors) and assignments (or assignees) in situations where such distinctions are significant.

visitor from a sensitive country begins, a national security background check must be completed to determine if appropriate U.S. government agencies have derogatory information, such as an intelligence affiliation, about that individual.

DOE also has security procedures that control the access of foreign visitors to the weapons laboratories. All foreign visitors—whether on a visit or an assignment—must wear an appropriate badge to obtain entry to various parts of a weapons laboratory. Furthermore, depending upon the facility involved, the days of the week and the hours during which the foreign national can actually be on site are restricted. Finally, guards and other security countermeasures are used to control access to those parts of the laboratories where classified work is conducted. Security forces and other countermeasures are also used to monitor and control access to the less protected, controlled areas known as property protection areas—which are not open to the general public and which may contain unclassified sensitive information—to ensure that this information is not compromised.

As an added line of defense, DOE and its laboratories operate counterintelligence programs to identify and mitigate the risk that sensitive information could be divulged to foreign countries. Among other things, the counterintelligence personnel conduct awareness programs to keep employees aware of the risk of foreign intelligence-gathering activities, brief and debrief employees who host foreign visitors, conduct assessments of foreign visitor activity, and disseminate relevant information throughout the DOE community. However, they have no approval authority for foreign visitors. The laboratories' counterintelligence programs do not conduct counterintelligence "operations," such as surveillance activities. Situations of concern are referred to the Federal Bureau of Investigation (FBI), which performs counterintelligence operations or investigations as necessary.

Concerns Exist About the Potential Compromise of Sensitive Information

The risk that classified or sensitive information may be compromised through foreign espionage is real and has been long-standing. Espionage against the weapons laboratories occurred as long ago as the 1940s when the Manhattan Project was developing the nation's first nuclear weapons. As documented in a 1996 Central Intelligence Agency (CIA) report that detailed recently declassified documents, key information on nuclear weapons was obtained from Los Alamos by the Soviet Union. In the 1980s and 1990s, there have been other espionage activities against DOE's

laboratories, but information on these incidents remains classified. DOE, laboratory, and other agency counterintelligence professionals briefed us on them, which included recent cases involving the possible theft or compromise of sensitive information in which foreign nationals at DOE's laboratories played a prominent role.

The large and increasing number of foreign nationals visiting DOE's laboratories has raised concerns about the potential compromise of classified information or other sensitive or proprietary information at these facilities. Counterintelligence professionals point out that (1) the laboratories have desirable assets in the form of classified information and unclassified but sensitive information; (2) access by foreign nationals, even for a short time, can provide the opportunity to identify and target laboratory information; and (3) repeated and long-term contact between laboratory personnel and foreign nationals can create relationships that foreign countries can use to obtain information. They add that the threat has become more complex because not only is information on nuclear weapons desirable to some foreign countries, but information and technology of economic benefit is of great importance to all countries. Consequently, the laboratories face the risk of economic espionage by enemies and allies alike.

Past unclassified work done by GAO and classified work by others have shown the risks of foreign visits and DOE's problems in controlling foreign visitors' presence at its laboratories. In 1988, we reported that major weaknesses existed in DOE's foreign visitor program and, as a result, suspected foreign intelligence agents and individuals from facilities suspected of conducting nuclear weapons activities had obtained access to the laboratories without DOE's prior knowledge.⁵ More recently, classified reports—in 1992 by an intelligence community interagency working group and in 1997 by the FBI—have pointed out basic problems with DOE's counterintelligence efforts regarding the presence of foreign nationals at DOE's laboratories.

DOE itself is concerned about the number of foreign visitors to its facilities and the potential threat of espionage they pose and has obtained additional funding to help its counterintelligence programs respond to this potential threat. Counterintelligence funding for headquarters program direction and field activities in fiscal year 1996 totaled about \$3.2 million. DOE was appropriated an additional \$5 million in fiscal year 1997 to expand

⁵Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31, Oct. 11, 1988).

counterintelligence programs at its nuclear weapons laboratories and other high-risk facilities.

Objectives, Scope, and Methodology

A May 7, 1996, report of the House Committee on National Security directed GAO to determine how well DOE is controlling foreign visits to DOE's three weapons laboratories and to determine whether these visits raise security or nuclear proliferation concerns. Since that time, we have issued to the Committee a Statement for the Record describing the number of foreign visitors to these laboratories and a report discussing the distribution of the fiscal year 1997 counterintelligence funds provided to DOE.⁶ This report completes our work on DOE's controls over foreign visitors and, as agreed with Committee staff, addresses DOE's (1) procedures for reviewing the backgrounds of foreign visitors and for controlling the dissemination of sensitive information to them, (2) security controls for limiting foreign visitors' access to areas and information within its laboratories, and (3) counterintelligence programs for mitigating the potential threat posed by foreign visitors.

To obtain an overall perspective on DOE's foreign visitor procedures, security controls, and counterintelligence efforts, we obtained and reviewed pertinent DOE and laboratory orders, documents, and other materials. We also met with and interviewed DOE headquarters, field office, and contractor officials, including officials from DOE's Offices of Defense Programs, Nonproliferation and National Security, and Policy and International Affairs in Washington, D.C., and in Germantown, Maryland, as well as officials at DOE's field locations in Albuquerque and Los Alamos, New Mexico, and in Livermore, California. We also met with contractor officials at the Lawrence Livermore National Laboratory in Livermore, California; the Los Alamos National Laboratory in Los Alamos, New Mexico; and the Sandia National Laboratories in Albuquerque, New Mexico. Furthermore, we met with officials from the FBI to obtain their views on the risk of, and control over, foreign visitors to DOE's laboratories.

In reviewing procedures on background checks for foreign visitors, we reviewed data on visits that occurred between January 1994 and December 1996. We examined records on visits and background checks contained in (1) DOE's centralized computer database on foreign visitors,

⁶DOE Security: Information on Foreign Visitors to the Weapons Laboratories (GAO/T-RCED-96-260, Sept. 26, 1996) and Department of Energy: Information on the Distribution of Funds for Counterintelligence Programs and the Resulting Expansion of These Programs (GAO/RCED-97-128R, Apr. 25, 1997).

(2) the laboratories' badging office and local foreign visitor databases, and (3) DOE's centralized counterintelligence database. We did not independently verify the accuracy of the information in these databases; however, we did obtain additional verification of visit information as necessary to complete our review. In particular, our analysis focused on the adequacy of DOE's controls related to high-risk visitors (i.e., visitors from sensitive countries who potentially could have derogatory national security information on file). In this regard, we tracked information on such visitors by examining DOE's records on background checks and by independently obtaining some background checks from the FBI.

To examine the process used for identifying sensitive subjects and controlling the dissemination of such information to foreign visitors, we obtained and analyzed pertinent guidance on sensitive subjects and discussed with DOE and contractor officials (including some who had hosted foreign visitors) the methods by which visits involving sensitive subjects are identified. We examined records on several hundred visits that occurred from January 1994 through December 1996. We judgmentally selected for further analysis over 150 visits that were not identified as involving sensitive subjects and compared the visits' purpose and/or subject with those identified on DOE's sensitive subject list. We discussed these visits with DOE officials in its Nuclear Transfer and Supplier Policy Division, which is responsible for reviewing visits that involve sensitive subjects, to obtain their perspectives on the accuracy of the identification of sensitive subjects. Additionally, we followed up with researchers and managers at these laboratories who frequently host foreign visitors concerning whether individual research projects that involved foreign nationals involved sensitive subjects.

To assess the security controls associated with foreign visitors' access to certain areas and information within DOE's laboratories, we obtained and examined security procedures, plans, surveys, and statements of threat. Our work included a review of laboratory security infractions, violations, and occurrences, as well as laboratory counterintelligence contact/incident reports. Additionally, we obtained unclassified program and building security assessments that identified problems and vulnerabilities. While touring laboratory facilities with security personnel, we observed the security controls in place for both classified and unclassified sensitive research.

To review the counterintelligence programs, we interviewed DOE, laboratory, and FBI counterintelligence officials and obtained pertinent

documentation regarding the potential threat posed by foreign visitors to the weapons laboratories and DOE's activities to counter this threat. In particular, we attended a classified counterintelligence briefing that was held for staff of DOE's Albuquerque Operations Office, which discussed the foreign visitor threat. We also examined the laboratories' counterintelligence contact/incident reports and observed the capabilities of DOE's centralized counterintelligence database. In addition, we obtained and reviewed assessments of DOE's counterintelligence programs that had been conducted by other organizations in the U.S. intelligence community.

We encountered two limitations in our attempts to examine DOE's controls over foreign visitors to its laboratories. First, our request to the CIA for access to data on the backgrounds of foreign visitors was denied on grounds of the sensitivity of the data. As a result, we were unable to review background information from the CIA that was on file at DOE or to independently obtain background data from the CIA. Second, we requested from the FBI specific information on possible espionage or other illegal activities at the laboratories. However, FBI officials told us that disclosure of such information is contrary to FBI policy; consequently, the requested information was not provided to us.

We provided a draft of this report to DOE for its review and comment. DOE's comments and our response are included at the end of chapter 5; the full text of DOE's comments are included in appendix IV. Our work was conducted from July 1996 through September 1997 in accordance with generally accepted government auditing standards. Major contributors to this report are listed in appendix V.

Foreign Visitor Procedures Have Not Been Effectively Implemented

Although foreign visitors provide many benefits to DOE's programs, every one of their visits to a nuclear weapons laboratory poses a risk that sensitive information might be inadvertently or intentionally compromised. To minimize this risk, DOE's foreign visitor order specifies several procedures that should be conducted before foreign nationals are allowed access to its laboratories. DOE has not effectively implemented two of the key procedures at the three laboratories we reviewed. More specifically:

- Few national security background checks are being performed on visitors from sensitive countries. As a result, foreign nationals suspected by the U.S. counterintelligence community of having foreign intelligence affiliations have been permitted access to the laboratories without the advance knowledge of appropriate officials.
- Because of unclear criteria regarding what constitutes sensitive subjects and the lack of an independent review process to examine the subjects to be discussed during visits, foreign visits involving potentially sensitive subjects—such as inertial confinement fusion, hydrodynamics codes,¹ and the detection of nuclear weapons tests—are occurring without DOE's knowledge.

Without adequate knowledge about the foreign nationals who plan to visit its laboratories and the subjects to be discussed during those visits, DOE cannot take appropriate action to ensure that their visits are properly controlled. This heightens the risk that such visitors may obtain, either directly through active intelligence efforts or indirectly through involvement in laboratory activities, information whose disclosure to certain countries would be detrimental to the United States.

DOE Has Little Advance Knowledge About the Backgrounds of Many Visitors From Sensitive Countries

Background checks can provide DOE and its weapons laboratories advance warning of possible problems or concerns with a foreign visitor, and DOE's foreign visitor order contains requirements for obtaining background checks for visitors from sensitive countries. However, DOE granted two laboratories—Los Alamos and Sandia—a partial exception from complying with its requirements. As a result, few background checks have been initiated for foreign visitors to those two facilities.

¹Among other things, hydrodynamics codes are used for computer simulations to model the dynamic processes that occur in a nuclear weapon.

**Background Checks Are
Intended to Help DOE
Mitigate the Risks of Visits**

As part of its process to approve foreign visitors, DOE requires that national security background checks (termed indices checks by DOE) be conducted on certain foreign visitors to its laboratories. Under DOE's order, background checks are required for all sensitive-country assignees (those whose visits will exceed 30 days). Additionally, background checks must be proposed by the laboratories to DOE's Counterintelligence Division for short-term visitors from sensitive countries, but the division has the discretion to determine whether the background check should be done. For example, the Counterintelligence Division may choose to request background checks on sensitive-country visitors who will be entering security areas or discussing sensitive subjects. The checks are obtained from government intelligence and investigative agencies, such as the CIA and the FBI. At DOE's request, these agencies review their files and report to DOE whether intelligence information of a derogatory nature exists about a particular visitor (e.g., that the visitor is suspected of having ties to a foreign intelligence service or terrorist group). DOE's order also requires that some background checks—those considered necessary to approve a visit or assignment—be completed before the visit or assignment begins. Many other checks done on visitors need not be completed before the visit begins—these are checks considered needed for counterintelligence research purposes only.

Although DOE uses the results of these background checks to approve proposed visits and to help mitigate any risks related to them, the existence of derogatory information about a foreign visitor does not preclude a visit from occurring. According to DOE officials, if a background check reveals derogatory information about a foreign visitor, the visit is rarely denied. Instead, DOE allows the visit to occur but, depending on the results of the check and other factors, may increase the stringency of escort requirements or may restrict the length of the visit, the buildings to be accessed, or the subjects to be discussed. Thus, the background check serves as means to forewarn DOE and laboratory officials of possible national security concerns so they may devise appropriate countermeasures where needed.

**Few Background Checks
Are Performed on
Sensitive-Country Visitors
to the Los Alamos and
Sandia Laboratories**

Few background checks are performed for visitors to DOE's Los Alamos and Sandia laboratories. In August 1994, these laboratories implemented a partial exception from the foreign visitor order that was granted by DOE. Under the terms of this exception, the two laboratories are required to request background checks only on those foreign visitors planning to enter a security area at the laboratory or to discuss sensitive subjects. According

to DOE and laboratory officials, the partial exception for Los Alamos and Sandia was granted because of the high volume of foreign nationals desiring to visit these weapons laboratories, which contributed to processing backlogs, and the costs associated with processing paperwork for foreign visitors. Laboratory officials said the processing backlogs caused delays that resulted in some visits having to be canceled because of uncompleted background checks.

The partial exception has limited the number of requests for background checks on visitors to Los Alamos and Sandia. As a result, DOE obtains relatively few background checks on visitors to those laboratories, particularly in comparison to Livermore, which did not request an exception from the order's requirements. Our review of DOE's records of foreign visitors showed that, during the 3-year period from 1994 through 1996, background checks were obtained on only 5 percent of the visitors from sensitive countries to Los Alamos and Sandia. In contrast, Livermore requested checks on many more names during that timeframe, and background checks were obtained on 44 percent of the visitors from sensitive countries to this laboratory.² Table 2.1 compares the number of background checks obtained on sensitive-country visitors for the three laboratories.

Table 2.1: Background Checks That Were Obtained on Sensitive-Country Visitors to DOE Weapons Laboratories, 1994-1996

Facility	Number of visits	Number of background checks	Percent checked
Los Alamos	2,714	139	5
Livermore	1,602	700	44
Sandia	1,156	53	5
Total	5,472	892	16

Source: Compiled by GAO from DOE and laboratory data.

Data on foreign visitors from individual sensitive countries also showed significant differences among the laboratories. For example, 46 percent of the Russian visitors to Livermore were checked during that 3-year period, compared to 10 and 7 percent, respectively, for Los Alamos and Sandia. Furthermore, 39 percent of the Chinese visitors to Livermore were checked, compared to 2 and 1 percent, respectively, for Los Alamos and Sandia. (See app. III for numbers and percentages for all sensitive countries.)

²In addition, some names reported to headquarters did not result in checks because previous check results were on file at DOE headquarters and still current.

By checking the backgrounds of so few visitors from sensitive countries, particularly to Los Alamos and Sandia, DOE limits the collection of basic counterintelligence data and may be unknowingly allowing significant numbers of visitors with questionable backgrounds into its weapons laboratories. According to FBI counterintelligence officials, the low percentage of background checks conducted on Russian and Chinese visitors to Los Alamos and Sandia does not constitute effective use of the background check process. Statistics on the results of background checks DOE did request support this. Of all the background checks DOE obtained on visitors from sensitive countries to the weapons laboratories during the 1994 through 1996 timeframe, about 4 percent of the checks that DOE received indicated the existence of derogatory information.

Moreover, we noted during our review that people with suspected foreign intelligence connections were let into the laboratories without background checks.³ We were able to document 13 instances where persons with suspected foreign intelligence connections were allowed access without background checks—8 visitors went to Los Alamos and 5 went to Sandia—during the 1994 through 1996 period.⁴ Available records also indicated that 8 other persons with suspected connections to foreign intelligence services were approved for access to Sandia during the period; however, DOE and Sandia lacked adequate records to confirm whether the persons actually accessed the facility. Although we could not confirm that any of these visits compromised U.S. security, at a minimum, the lack of a background check did not provide DOE the opportunity to implement countermeasures to mitigate the potential risk posed by these visits. Also, all of these instances occurred at the two weapons laboratories that had been granted a partial exception to DOE's foreign visitor order.

DOE's requirements for national security background checks represent a continuing problem that we previously identified in a 1988 GAO report⁵ and about which elements of the U.S. intelligence community have also expressed concern. In discussing this problem, DOE and laboratory counterintelligence officials said that they recognize that the number of background checks obtained on foreign visitors has been limited, especially at Los Alamos and Sandia, and that these checks should be

³Despite the restrictions on our access to information, as discussed in chapter 1, we verified through the U.S. counterintelligence community that several of these visitors had known or suspected connections with foreign intelligence services.

⁴We also identified instances of persons with suspected intelligence connections obtaining laboratory access before background checks were completed.

⁵GAO/RCED-89-31, Oct. 11, 1988.

routinely requested for visitors from sensitive countries. They added that although data from a background check—even derogatory data—is rarely used to deny a visitor access to a laboratory, obtaining such information is beneficial in identifying individuals known to be a risk. DOE headquarters counterintelligence officials said their long-term goal is to obtain background checks on all foreign nationals from sensitive countries that seek to visit any of these three laboratories. In the interim, according to a Sandia counterintelligence official, that laboratory is now reporting data on all sensitive country visitors to DOE headquarters for potential background checks.

DOE Has Not Adequately Ensured That Visits Involving Sensitive Subjects Are Identified and Reviewed

DOE has little assurance that all visits during which sensitive, but unclassified, subjects will be discussed are identified and brought to the attention of DOE officials. According to DOE's order, DOE officials are to review and approve visits by foreign nationals that involve sensitive subjects. But DOE and laboratory personnel alike are unclear about what constitutes a sensitive subject, and little or no independent review takes place to assess subjects within the context of the planned visit (e.g., taking into account the purpose of the visit, the particular aspects of the subject to be discussed, and the foreign country and individuals involved). As a result, sensitive information could be discussed or otherwise disclosed to foreign nationals without DOE's knowledge and approval.

DOE Requires the Identification, Review, and Approval of Visits Involving Sensitive Subjects

To minimize the risk of inappropriate subjects being discussed with foreign nationals, DOE's order requires that its laboratories identify any visit involving a sensitive subject for review and approval by DOE. The order defines sensitive subjects as unclassified subjects involving information, activities, or technologies relevant to national security. To facilitate their identification, the order contains a list of sensitive subjects, including nuclear weapons production and supporting technologies, nuclear explosion detection, inertial confinement fusion, production and handling of plutonium, and fuel fabrication. Additionally, the order contains three criteria for identifying other subjects that may be sensitive. Subjects are considered sensitive if they relate to technologies under export control, "dual-use" technologies that have both peaceful and military applications, or rapidly advancing technologies that may become classified or placed under export control. Subjects in these categories include computer systems, component development, and software specifically designed for military applications; extremely high-energy,

high-brightness lasers and particle beams; and high energy density batteries and fuel cells.

The responsibility for reviewing visits involving sensitive subjects rests with DOE's Nuclear Transfer and Supplier Policy Division in the Office of Arms Control and Nonproliferation. This division also reviews private-sector exports of information and technology that could be useful to a foreign nuclear or nuclear weapons-related program. According to division officials, while the discussion of a sensitive subject with a foreign national is not necessarily prohibited, DOE needs to be aware of any such discussions to ensure their consistency with U.S. policy regarding the transfer of that information to the foreign national's home country. The officials added that the need for DOE's review and approval of the discussion of a sensitive subject is not dependent on the visitor's home country—the discussion of any sensitive subject with a foreign visitor from even a nonsensitive country still requires DOE's review and approval.

Identification of Visits That Involve Sensitive Subjects Has Not Been Adequate

DOE's three weapons laboratories have not adequately identified visits involving sensitive subjects. Between January 1994 and July 1996, they identified a total of 72 visits involving sensitive subjects; the majority of these visits were related to areas specified as sensitive in DOE's order. For example, 5 Russian citizens visited Los Alamos in 1994 for a 3-day visit involving nuclear materials control, accounting, physical protection, security, export control, and critical assembly facilities; 13 Russian nationals visited Los Alamos in 1995 for a 1-day workshop on plutonium stabilization, storage, and disposition; and 30 French nationals visited Livermore in 1995 for 1- to 2-year assignments to work on inertial confinement fusion.

However, our review of records on 167 other visits found numerous cases that pertained to subjects that were either specified as sensitive in DOE's order or were potentially sensitive but were not identified as such by the laboratories. For example:

- Sixteen visits and assignments to Livermore involved inertial confinement fusion, a technology specifically listed as sensitive in DOE's order. These visits included foreign visitors who were participating in a formal bilateral cooperative effort, including the transfer of proprietary data, between the United States and France on subjects related to inertial confinement fusion. On other occasions, Livermore has identified this type of visit as involving a sensitive subject.

- A Canadian citizen was on an assignment to Livermore to discuss equation of state measurements⁶ using laser-generated shock-waves—work that was acknowledged to be important to the inertial confinement fusion program, a sensitive subject area.
- An Indian citizen from a defense-related facility in India was on an assignment to Los Alamos that involved the structure of beryllium compounds. Beryllium metal is used in nuclear weapons.
- An Indian citizen was on assignment to Los Alamos for work related to pattern recognition/anomaly detection algorithms. This work was acknowledged to be dual use in nature, with applications related to national security, such as nonproliferation and satellite image processing, as well as to nondefense projects.
- A Russian visit to Los Alamos involved collaboration on processes related to detecting unsanctioned nuclear weapons tests. Nuclear explosion detection is specifically identified as a sensitive subject in DOE's order.
- A citizen of the United Kingdom was assigned to Livermore for 3-dimensional hydrodynamic simulations for implosions. Hydrodynamics and 3-dimensional calculations are important to simulating nuclear weapons tests, particularly in light of the ban on nuclear testing.

We reviewed copies of the documentation on these visits and discussed them with officials in DOE's Nuclear Transfer and Supplier Policy Division to obtain their perspectives on whether they may have involved sensitive subjects. They said that it was not possible to fully ascertain whether these visits did or did not involve sensitive subjects; however, they pointed out that many of them appeared to involve subjects that are specifically identified as sensitive subjects in DOE's order and that others appeared to have some weapons or dual-use applications. The export control officials said that, according to the stated purpose of the visits described in their documentation, they involved subjects that should have been sent for their review.

Problems Hindering the Identification of Visits Involving Sensitive Subjects

DOE's weapons laboratories have had problems identifying visits involving sensitive subjects largely for two reasons—confusion over how to apply the sensitive subject criteria and the lack of an independent technical review of proposed foreign visits to identify those involving sensitive subjects.

According to laboratory program managers and hosts of foreign visitors, DOE's criteria for identifying sensitive subjects are very broad and do not

⁶Equation of state measurements are used to assess how materials interact with their surroundings.

clearly define which activities are covered. The laboratory managers added that the current list of sensitive subjects is outdated, incomplete, and does not establish reasonable parameters within which they could reasonably gauge a subject's sensitivity. As an example of the difficulty in applying the criteria, they noted that while inertial confinement fusion is listed as a sensitive subject because of its relationship to nuclear weapons testing, most aspects of this technology are unclassified and widely researched throughout the world and that the laboratory's unclassified inertial confinement fusion work is published and freely disseminated. They added that without more specific criteria from DOE, they generally view activities in inertial confinement fusion and other areas that are unclassified, already published, or will ultimately be published, to be nonsensitive.

DOE officials with the Nuclear Transfer and Supplier Policy Division acknowledged that although there are difficulties in identifying sensitive subjects, the laboratories are interpreting the order's criteria too narrowly. They said that the sensitivity of a subject may at times be subjective and it often depends on the country to which the information will be divulged, the state of that country's technology and research efforts, and other information on that country's needs and intentions regarding the use of the technology. However, they added that hosts are not in a position to know that information and/or whether it is consistent with U.S. government policy to provide that information to the country in question. The list of sensitive subjects serves as a guideline to identify such visits for scrutiny by DOE officials who possess the necessary expertise to determine whether it is appropriate to discuss a particular subject with a foreign visitor from a specific country.

A second problem hindering the identification of visits involving sensitive subjects is the lack of an independent review of proposed visits by individuals with technical expertise to help ensure sensitive subjects are properly identified. During the period of our review, DOE and the weapons laboratories relied upon the host—the laboratory employee sponsoring the foreign visitor—to accurately identify sensitive subject visits. Such visits were approved by the appropriate laboratory division management and by officials in the foreign visits and assignments office at each laboratory. However, little or no independent review of the subject of those visits had been conducted to ensure that sensitive subjects were not involved. At Sandia and Los Alamos, officials in the foreign visits and assignments office review requests for foreign visitor access; however, those individuals do not have a technical background or expertise to judge if a

sensitive subject is involved. At Livermore, visit requests are reviewed in the office of the laboratory director, as well as at the DOE operations office; however, this laboratory's review has at times been delegated to individuals from the foreign visits and assignments office. Laboratory personnel from the foreign visits and assignments offices told us that they are not fully knowledgeable on activities that could be sensitive and that they generally rely on the host to determine whether a visit would involve a sensitive subject.

DOE and Laboratories Recognize Problems With Identifying Visits Involving Sensitive Subjects

DOE and the weapons laboratories have recognized problems with identifying visits involving sensitive subjects and have begun actions to address them. In the fall of 1996, DOE initiated a multiissue effort to revise its foreign visit and assignment order. This effort will include examining the controls over foreign visits involving sensitive subjects and developing a better process and/or criteria by which to identify them. According to officials in DOE's Counterintelligence Division, which is involved in the effort, the revised order is expected to be issued by the end of 1997. However, because revision of the criteria for identifying sensitive subjects has not yet gotten underway and does not have a timetable for completion, they do not know if changes to clarify DOE's criteria for identifying visits involving sensitive subjects will be included in the revised order.

During our review, two of the three laboratories established interim local processes to examine requests for foreign visitors to better ensure that their visits do not involve discussions of sensitive subjects. In August 1996, Livermore began requiring that all visits involving foreign nationals from sensitive countries be reviewed by an official in its Arms Control and Treaty Verification Program who has had experience with nuclear weapons and associated technologies. These reviews are specifically to assess the technology involved and identify those requests that involve sensitive subjects. According to the Livermore official conducting these reviews, although most visits have not involved sensitive subjects, he has identified some visits of concern, for which actions were taken to help ensure that sensitive subjects would not be involved. In December 1996 Sandia began requiring that all requests for foreign visitors be reviewed by a Sandia official involved in export control to better ensure visits involving sensitive subjects are adequately identified.

Security Controls May Not Adequately Protect Sensitive Information From Foreign Visitors

Effective security controls can greatly mitigate the risk inherent with the presence of foreign visitors at DOE's weapons laboratories. However, the security controls that exist in the laboratories' controlled areas—the areas most often visited by foreign nationals—may not provide effective protection. The controlled areas contain unclassified, but sensitive information, and although security measures are used to control access, these measures are less stringent than those used in classified areas and their implementation varies among the laboratories. Security problems and vulnerabilities involving foreign nationals show that classified and/or sensitive information has been, or potentially could be, compromised by foreign nationals in the controlled areas. Nevertheless, DOE has not fully assessed the effectiveness of its security measures to protect sensitive information in controlled areas.

Security Requirements in Controlled Areas

To protect information from unauthorized disclosure or compromise, DOE and its laboratories use various levels of security that permit access for authorized individuals to certain areas. Although some foreign visitors are allowed access to the more restrictive security areas where classified work is conducted, most foreign visits occur in designated controlled areas—often termed property protection areas—which may contain unclassified sensitive information. A lower level of security is provided in these areas, and the controls used vary among the laboratories.

Most Foreign Visitors Work in Controlled Areas

DOE and the laboratories use a multilevel, graded security approach to limit access and protect information at their facilities. Open areas, which include locations on laboratory property to which the general public is allowed access, receive a low level of protection. Open areas can include cafeterias, visitors centers, and museums. Controlled areas, which receive a higher level of protection, can include small areas, such as an individual building, as well as larger areas, such as building complexes. Access to these areas is controlled because of the presence of valuable property or unclassified sensitive information, but no classified work is conducted in these locations. Unclassified sensitive information includes information that has been designated Official Use Only, proprietary, export controlled, Privacy Act, and Unclassified Controlled Nuclear Information.

An even higher level of protection and stricter access limitations are maintained for security areas containing classified information and technologies or in which nuclear weapons or other classified research is conducted. These areas are closely monitored and patrolled, and controls

traditionally include guns, guards, and gates. Specific security plans must be developed and approved before any foreign visitor is allowed access to these areas and the visitor must be escorted at all times.

Most foreign visitors to the weapons laboratories are granted access to the controlled areas. Laboratory records show that on average only about 5 to 10 percent of all foreign visitors are permitted into security areas where classified work is performed, and according to DOE and laboratory officials, such access is usually for a short period of time. The remaining visitors are either allowed into the controlled areas or meet with laboratory employees in open areas. DOE and laboratory officials were not able to identify the percentage of those visitors that went to controlled areas, but stated that most were allowed into these locations.

Security Controls Vary Among the Laboratories

Because valuable property and information that is unclassified, but sensitive, is located in controlled areas, DOE requires the laboratories to protect these areas through the use of a variety of security controls. Controls used to reduce the risks posed by foreign nationals in controlled areas include the following:

- A distinctive identification badge must be worn by foreign visitors at all times.
- Access is controlled by automated devices or by receptionist staff and manual visitor logs. Automated devices include equipment that reads encoded access cards and/or requires passwords.
- Standard or "generic" security plans are drafted for controlling foreign visits in the area.
- A host is designated, who is a laboratory employee responsible for the activities of the foreign national while at the laboratory. A visitor or assignee is not permitted to be a host.
- Random searches are conducted on vehicles or hand-carried items entering or leaving the area.

Among the three laboratories, however, the security controls associated with foreign visitors in controlled areas are not consistently applied. In particular, each of the laboratories has different requirements for allowing foreign visitors after-hours access. At Livermore, foreign visitors are not allowed unescorted after-hours access to controlled areas without the specific written approval of laboratory security officials and the concurrence of the local DOE field office. According to Livermore security officials, while they have granted such access for some foreign visitors,

they do not approve unescorted after-hours access for visitors from sensitive countries.

At both Los Alamos and Sandia, unescorted after-hours access to controlled areas has been permitted. These laboratories have required the host to monitor the foreign visitor—that is, be aware of the foreign visitor's location and activities—but not necessarily be physically present. Recently, Sandia revised its after-hours access policy. In November 1996, Sandia no longer allowed foreign nationals to have unescorted after-hours access to controlled areas without the approval of its counterintelligence office. According to Sandia and DOE officials, this change was made because of the potential for security problems that could result from unescorted access. Los Alamos, however, continues to allow unescorted after-hours access to preserve what one official described as an open "campus atmosphere" for researchers at its facilities.

Laboratory policies also vary regarding random searches in controlled areas and the appearance of foreign visitor identification badges. While all of the laboratories officially permit random searches in controlled areas, at one of the laboratories such searches are discouraged during normal work hours. Additionally, the distinctive color and wording of badges for foreign visitors differ among the laboratories. For example, at Livermore those badges are white (for visits) or red (for assignments), at Los Alamos badges for foreign visitors are red, and at Sandia those badges are gray. Furthermore, unlike the badges at the other laboratories, Sandia's badges contain no wording pertaining to the visitors' countries of citizenship or indicating that the wearers are not U.S. citizens.

Finally, neither Los Alamos nor Sandia has developed security plans—even generic ones—for foreign nationals who will be in controlled areas. The DOE order governing unclassified foreign visits and assignments identifies security plans as the basic means by which vital information is protected and requires they be developed. However, DOE and laboratory officials told us that because of the exception granted by DOE to these two laboratories—which also streamlined requirements for background checks and visit approvals—security plans are no longer required for visits to controlled areas. Livermore has not sought such an exception and requires a generic security plan for all foreign visitors to its controlled areas.

Security Vulnerabilities and Problems Have Involved Foreign Visitors

Available data from the weapons laboratories showed that the sensitive information in controlled areas has been vulnerable to compromise. Between 1991 and 1997, laboratory security assessments and records identified vulnerabilities and problems involving foreign visitors, and in buildings and programs to which those visitors had access. Records of vulnerabilities and problems included improper releases of information and failures to follow security controls and requirements.

Improper Releases of Information

Assessments and records from all three laboratories indicated vulnerabilities and problems involving the improper release of unclassified sensitive information and classified information in unclassified settings. In most of these cases, the information was actually or potentially available to foreign visitors. Whether or not a laboratory employee personally hosts a foreign visitor, all laboratory employees must adequately protect classified or unclassified sensitive information and not disclose it unless authorized. However, examples of improper releases included the following:

- Unclassified sensitive documents and materials had been improperly discarded in trash, recycling bins, or hallways. At one of the laboratories, six boxes of papers marked "sensitive material" in red letters on the outside were left in an open hallway in an area accessible to foreign visitors.
- At one of the laboratories, a division's open-access newsletter, which was accessible to the foreign visitors it was hosting, provided information on corporate and laboratory research agreements, the development of certain computer codes, and DOE's nuclear program.
- Classified information had been inadvertently divulged by laboratory employees during unclassified workshops or conferences to foreign visitors, some of whom were from sensitive countries.
- A departmental newsletter containing classified information was sent to 24 uncleared individuals, 11 of whom were foreign visitors. Some of the foreign visitors were from a sensitive country.

Failures to Follow Security Requirements and Controls

Vulnerabilities and problems associated with employees' failures to follow security requirements and controls were also identified in the laboratories' records. The following are several examples:

- In one case, a laboratory employee in a building to which foreign visitors had access failed to question the unauthorized removal, by members of a security assessment team during a test exercise, of a complete computer

system from a controlled area. The employee did not challenge the team's activities despite the fact that its members were not wearing identification badges and were openly discussing plans to remove additional machines and equipment in an effort to appear suspicious.

- On 10 separate occasions, a laboratory employee hosted visitors from sensitive countries without following visit approval requirements or gaining appropriate authorizations prior to those visits. Another host at the same laboratory met foreign visitors off-site without proper approval after a laboratory official advised him that he could "receive a reprimand, but it would not jeopardize his security clearance."
- In another case, a host, when confronted with a requirement to limit after-hours laboratory access of certain sensitive country assignees assisting him with his research, moved the visitors and his research to an off-laboratory location.
- On several occasions, there were miscellaneous failures to follow security procedures, including computers left on and unattended without password protection, improper escorting of foreign visitors who required such oversight, and unauthorized back door entry to controlled areas where many foreign visitors had access.

DOE and laboratory security officials told us that they are concerned about, but not surprised by, vulnerabilities and problems in controlled areas. The openness under which unclassified research programs operate poses a dilemma in an age of economic competitiveness. DOE's own security awareness literature states that although many employees realize the importance of protecting classified information, few are aware of the significance of unclassified sensitive and proprietary information. Furthermore, DOE and laboratory security officials told us that the security consciousness of employees working in controlled areas is more relaxed than in security areas where classified research is conducted. While some security officials said that they would like to see a stronger emphasis on security in controlled areas at the laboratories, others said that some technical and research staff do not place a high priority on security and actually see it as an impediment to their work.

Protection of Sensitive Information in Controlled Areas Has Not Been Fully Assessed

Neither the laboratories nor DOE has fully assessed the controls over unclassified, but sensitive information. At the laboratories, operations security (OPSEC) assessments are performed to identify vulnerabilities. However, only at Sandia has there been an assessment that specifically focused on controls over unclassified sensitive information in controlled areas to which foreign visitors have access. Furthermore, while DOE has assessed overall laboratory security operations on a regular basis, its

assessments have not addressed the protection of unclassified sensitive information in controlled areas.

DOE requires the use of OPSEC techniques and measures to help protect information and activities related to national security and government interests. The purpose of OPSEC is to disrupt or defeat the ability of foreign intelligence or other adversaries to acquire sensitive or classified information and to prevent the unauthorized disclosure of such information. Each of the laboratories has an OPSEC program and uses OPSEC assessments to identify security vulnerabilities associated with specific laboratory facilities or programs. To identify vulnerabilities, OPSEC personnel assess various practices, including physical security and access controls; visitor log and escort procedures; availability of sensitive information on bulletin boards, in meeting rooms, and in offices; document disposal and destruction methods; and computer access protections.

While all three laboratories have performed OPSEC assessments, only Sandia has conducted an assessment specifically focused on controls over unclassified sensitive information in controlled areas to which foreign visitors have access. Sandia's assessment was completed in March 1997, and although it found no indication that the laboratory had allowed foreign visitors to compromise proprietary or sensitive information, it concluded that Sandia needed to define a policy concerning areas and information sources to which foreign nationals should have access. Subsequently, Sandia changed the process for controlling foreign visitors' access to, and work in, controlled areas. Foreign nationals visiting Sandia for more than 30 days now work in "export controlled zones"—locations within controlled areas where they can work with their respective project teams but are restricted from unauthorized access to research in the surrounding area.

OPSEC assessments at Livermore or Los Alamos have not yet examined foreign visitors' access to sensitive information. Livermore's past OPSEC assessments have dealt with visitors in general, but have not specifically addressed foreign visitors and the potential for them to access sensitive information. Livermore's OPSEC manager said that the laboratory plans to conduct two such assessments before the end of 1997. Similarly, Los Alamos' OPSEC assessments have included some issues related to foreign visitors, such as their access to open and secure areas, but they have not focused on assessing whether foreign visitors could obtain sensitive information.

In addition to the laboratories' OPSEC assessments, DOE does broader periodic surveys of their security operations, including visits and assignments involving foreign nationals that are intended to be comprehensive assessments of each laboratory's security operations. Generally, DOE's surveys are performed every year or two, depending on the findings of the previous survey for a specific laboratory. The most recent surveys at Los Alamos and Sandia were completed in March and April of 1997, respectively. The most recent survey of Livermore's program was completed in August 1996. In these surveys, each of the laboratory's foreign visits and assignments program was rated satisfactory. However, the primary focus of these surveys was on the program's organization, management, and operations, and not on information protection. As a part of DOE's past surveys, each laboratory's program was evaluated by conducting interviews, reviewing documentation, and testing performance. The surveys did not address protection of unclassified sensitive information in controlled areas—in general or in association with foreign visitors. For example, while several sections in the survey report on security at Livermore addressed the effectiveness of its controls over classified information, none addressed the adequacy of protections for unclassified sensitive information.

DOE's Counterintelligence Efforts Can Be Improved

DOE's headquarters and field counterintelligence programs are an important part of its defense against foreign espionage efforts at the nuclear weapons laboratories. Foreign visitors to these laboratories have open, often long-term, access to personnel with detailed knowledge and expertise in classified and/or sensitive matters. Although this situation is viewed by counterintelligence experts as an ideal opportunity for foreign intelligence-gathering efforts, DOE has not comprehensively assessed the threat of foreign intelligence against the laboratories. A thorough assessment that identifies countries of concern, the technologies and the information these countries are seeking, and the programs that are likely to be targets of foreign intelligence, is important for DOE and its laboratories to understand and reduce the dangers posed by foreign visitors. Furthermore, DOE has not developed any meaningful programmatic measures by which to evaluate the effectiveness of the laboratories' counterintelligence programs nor has it periodically evaluated them. Recently, DOE initiated several actions to strengthen the counterintelligence programs, both at headquarters and at the laboratories.

DOE's Headquarters and Laboratory Counterintelligence Programs

The mission of DOE's counterintelligence programs is to implement effective defensive efforts departmentwide to deter and neutralize foreign government or industrial intelligence activities in the United States directed at or involving DOE. DOE's headquarters Counterintelligence Division, within the Office of Energy Intelligence, has overall responsibility for this mission and counterintelligence activities throughout DOE. Staffed with seven DOE employees and seven contract employees, DOE's Counterintelligence Division is responsible for such activities as conducting various threat assessments and identifying foreign intelligence activities directed against DOE as well as overseeing each laboratory's counterintelligence program. DOE's threat assessments can vary from a comprehensive threat assessment DOE-wide to a narrowly focused threat assessment that examines a specific issue, such as a particular foreign country's interest in DOE's assets. DOE's Counterintelligence Division is responsible for implementing counterintelligence policies and procedures throughout DOE. This responsibility includes (1) developing and implementing methods, techniques, standards, and procedures for DOE's counterintelligence activities; (2) establishing a briefing and debriefing program for foreign

travel and contacts; and (3) monitoring visits and assignments of foreign visitors to all of DOE's facilities.¹

Each laboratory has its own counterintelligence program, which is conducted in compliance with DOE's requirements, and laboratory counterintelligence officers report directly to laboratory management. The laboratories' programs emphasize employee briefings and debriefings as well increasing employees' awareness and knowledge about counterintelligence. Briefings and debriefings of employees take place prior to and/or after an event (e.g., when hosting a foreign visitor or when taking a foreign trip). In briefings, counterintelligence officers provide information to employees on such concerns as the types of subjects to avoid discussing with foreign visitors. In debriefings, these officers obtain information from the employees that can help DOE determine if there are indications that intelligence services are trying to target that laboratory or its staff.² Additionally, counterintelligence activities at each laboratory include initial investigations of possible foreign intelligence efforts to determine if referral to appropriate federal agencies would be warranted, liaison with federal agencies, and gathering and recording such basic counterintelligence information as foreign visitors' activities at a laboratory and persons contacted.

DOE officials estimate that operating the headquarters counterintelligence program costs about \$1.8 million annually. For fiscal year 1996, DOE's three weapons laboratories had a total counterintelligence program funding of \$905,000 and 9.4 counterintelligence staff years—funding of \$552,000 and 5.5 staff years at Livermore, funding of \$100,000 and 1.1 staff years at Los Alamos, and funding of \$253,000 and 2.8 staff years at Sandia.³

¹In addition, DOE field offices have counterintelligence program managers who are responsible for conducting a counterintelligence awareness program and providing briefings and debriefings related to foreign visitors and foreign travel.

²Briefings and debriefings are not conducted for all events; counterintelligence officers judgmentally sample from the universe of events, according to such factors as the visitor's country of origin or the subjects to be discussed.

³Numbers for Sandia include its laboratories in New Mexico and California.

DOE Has Not Clearly Defined the Threat Posed by Foreign Visitors to Its Laboratories

To understand the dangers posed by foreign visitors, DOE needs to perform a comprehensive assessment of the threat to its laboratories by foreign intelligence services. According to DOE and the FBI, the operation of an effective counterintelligence program is predicated upon a realistic and comprehensive examination of the foreign intelligence and insider threats. For example, according to the FBI, only a comprehensive threat assessment can address the issue of whether foreign intelligence services are making a concerted effort to target DOE laboratories, and if so, how they can work together to counter the threat. This threat assessment can also provide senior managers with an analysis of the global threat and the information and technologies at DOE and the laboratories that are most at risk.

Specific assessments, which are targeted studies that focus on country-specific issues, and annual foreign visitor statistical studies are also important because they can inform the laboratories about items of counterintelligence concern. This information can then be used by counterintelligence officers at each laboratory to mitigate the potential risk to that laboratory and its employees. For instance, information contained in these studies can be used to alert a laboratory's senior management and staff during briefings.

While DOE officials recognize the importance of both types of assessments, DOE headquarters' counterintelligence analysis has focused on the specific-type assessments and has not addressed the overall threat to its facilities. In recent years, DOE has done about 25 specific assessments, which have examined specific threats or, in some cases, have been statistical studies. For example, DOE has assessed the threat of Russian organized crime to DOE and Pakistan's access to DOE's resources. In many cases, such studies were based on the work of other agencies, such as the CIA or FBI, or were contracted out. While these studies can be useful in identifying a threat on a single issue, they do not relate the global foreign intelligence threat to the local situation at a specific weapons laboratory.

DOE counterintelligence officials at headquarters said that they need to do a comprehensive threat assessment that relates the global foreign intelligence threat to the laboratories, but they have been limited in their ability to do so. They said that specific threat assessments have had a higher priority because these studies meet the more immediate needs of the laboratories. Moreover, DOE's Counterintelligence Division has not had the staffing or analytical expertise required for this effort. In this regard,

DOE's counterintelligence officials said that they will need to rely on information from other agencies to do a comprehensive threat assessment.

Recognizing the need for a comprehensive threat assessment, in the fall of 1996 the then Deputy Secretary of Energy directed each of the weapons laboratories to conduct its own threat assessment, which DOE would then use to develop an overall, comprehensive threat assessment. Although the laboratories are in the process of completing their site threat assessments, according to a DOE counterintelligence official, the Department may not be able to develop a comprehensive assessment unless its priorities change and DOE receives assistance from the U.S. intelligence agencies in obtaining the sensitive intelligence information that is critical to develop this assessment.

DOE Has Not Effectively Overseen the Laboratories' Counterintelligence Programs

Oversight of the laboratories' counterintelligence programs and their activities—particularly setting expectations for program performance and periodically evaluating it—is one of the major responsibilities of DOE's Counterintelligence Division. However, DOE has not developed meaningful performance measures or expectations for the laboratories' counterintelligence programs or conducted periodic evaluations of them. DOE's oversight, however, has been hampered, in part, because the funding for their programs has been through laboratory overhead accounts instead of directly from DOE.

Meaningful performance measures for the laboratories' counterintelligence programs are important because they would help gauge whether or not those programs are achieving their intended purposes. According to DOE Order 5670.3, Counterintelligence Program, DOE is responsible for developing and implementing performance measures for counterintelligence activities throughout the Department. However, according to a counterintelligence official at headquarters, DOE has not developed any performance measures or expectations to evaluate the laboratories' counterintelligence programs because DOE's contracts with the laboratories do not obligate their counterintelligence programs to follow any such measures DOE may develop. According to this official, DOE is considering both amending those contracts to address this problem and issuing guidance and policy to define performance measures and expectations for the laboratories to follow and be evaluated against. This will be done after DOE completes its comprehensive threat assessment.

DOE's periodic evaluations of the laboratories' counterintelligence programs are also important because they help provide assistance to each laboratory as well as determine the effectiveness of their programs. DOE's counterintelligence order requires that the headquarters Counterintelligence Division oversee the implementation of counterintelligence policy and procedures at the laboratories. However, officials from that division could identify only one review it has conducted at the weapons laboratories, which occurred in 1996 in the form of a "staff assistance visit" conducted at Los Alamos. DOE concluded from this visit that because of inadequate staffing, Los Alamos' counterintelligence program was not comprehensive and only minimally accomplished the requirements of DOE's counterintelligence order. At that time, Los Alamos had one counterintelligence officer.

Livermore and Sandia have not had their counterintelligence programs reviewed by DOE headquarters. According to a DOE official, evaluations at Livermore and Sandia have not occurred because of other higher-priority work, such as the specific type of threat assessments mentioned earlier. In addition, they said that DOE cannot require its laboratories to implement any recommendations that might result from such evaluations. Without periodic evaluations of all their counterintelligence programs, assessing their effectiveness and objectively comparing one program with another will be difficult.

One factor that makes control by DOE headquarters over the laboratories difficult is that the counterintelligence programs are not funded directly by DOE's Counterintelligence Division. Until recently, each laboratory's program has been funded entirely from that laboratory's funds and, consequently, each laboratory operated its program autonomously. Accordingly, each laboratory's commitment to its program has differed, as illustrated by the difference in staffing levels. For example, while Livermore's counterintelligence program had 5.5 staff years in 1996, Los Alamos' program had only 1.1 staff years, despite having almost twice as many visitors from sensitive countries.⁴

According to the FBI, which has examined DOE's counterintelligence program, the structure of DOE and its relationship with contractor-operated laboratories have resulted in their having assumed a high degree of autonomy. This has resulted in a gap between authority and responsibility, particularly when national interests compete with the specialized interests

⁴Although both laboratories had equivalent numbers of foreign visitors (about 2,800), Los Alamos had nearly 1,000 visitors from sensitive countries, while Livermore had about 550 such visitors.

of the academic or corporate management that operate the laboratories. Furthermore, the FBI found that this autonomy has made national guidance, oversight, and accountability of the laboratories' counterintelligence programs arduous and inefficient. Moreover, DOE's Counterintelligence Division lacks direct management oversight and control to ensure the laboratories comply with its policies. This frequently puts the each laboratory's counterintelligence staff in an awkward, if not difficult, situation of dividing their loyalties between the interests of the laboratory in pursuing cutting-edge research and development and the need to safeguard U.S. national security interests.

DOE Is Taking Steps to Strengthen Its Counterintelligence Program

DOE has recently recognized that its counterintelligence program has been inadequate and has taken steps to strengthen it. The Congress appropriated \$5 million to DOE in counterintelligence funding for fiscal year 1997 in addition to its budget request, and DOE has used much of these funds to support the counterintelligence programs at the weapons laboratories.⁵ In November 1996, DOE's Deputy Secretary expressed concerns about the presence of foreign visitors at the laboratories, and as a result, several departmentwide corrective actions are now underway.

In the spring of 1996, the director of DOE's Office of Energy Intelligence briefed the staff of several congressional committees about the concerns raised by the increasing number of foreign visitors to its laboratories and the threat they posed. In the fall of that year, the Congress provided DOE with an additional \$5 million for fiscal year 1997 to expand counterintelligence activities at its weapons laboratories and other high-risk facilities. Of the \$5 million, about half—\$2.47 million—went to the three nuclear weapons laboratories.⁶ The additional funds were used to increase the number of counterintelligence staff at those laboratories and for counterintelligence-related analyses. As a result, DOE has increased the counterintelligence staff at the weapons laboratories.

On November 21, 1996, the then Deputy Secretary of Energy initiated several corrective measures to improve DOE's foreign visitors program. The Deputy Secretary met with officials of five DOE facilities: the three

⁵On April 25, 1997, we reported to the Committee about DOE's use of the \$5 million. Department of Energy: Information on the Distribution of Funds for Counterintelligence Programs and the Resulting Expansion of These Programs, GAO/RCED-97-128R.

⁶An additional \$1.27 million went to five other facilities; the remainder (\$1.26 million) was spent on counterintelligence analysis and assessment studies. When the \$5 million was made available, however, some facilities reduced or eliminated the funding they had previously provided for counterintelligence and over \$1 million was allocated to facilitywide support costs.

weapons laboratories, the Oak Ridge National Laboratory, and the Pacific Northwest Laboratory. Among the corrective measures the Deputy Secretary and these officials agreed to complete during fiscal year 1997 were the following:

- Develop training in export control and provide that training to laboratory staff at those five facilities.
- Develop new guidance on unclassified, but sensitive, subjects (i.e., matters unsuitable for discussion with a foreign visitor).
- Develop laboratory threat assessments of foreign visits and assignments.
- Develop a DOE-wide comprehensive threat assessment of foreign visits and assignments.

However, counterintelligence officials at headquarters expressed concerns about DOE's ability to complete these initiatives because DOE has historically given its counterintelligence program a low priority and the tendency for the laboratories to resist headquarters management. They said that they are hopeful that DOE's current Secretary will support these initiatives in the counterintelligence program.

Conclusions and Recommendations

With the end of the Cold War, DOE's nuclear weapons laboratories have been moving away from secret research toward more open and cooperative research with a variety of nations and an increasing number of foreign nationals. Open collaboration can greatly benefit DOE and the United States by stimulating the exchange of ideas and promoting cooperation. This in turn can lead to more efficient research and increase the likelihood of important scientific discoveries. While recognizing that such cooperation is beneficial, it is important to note that foreign espionage efforts against DOE's weapons laboratories may be more active than ever. Furthermore, these efforts may have expanded to include industrial espionage. All of this puts new burdens on DOE's security.

To respond to these challenges, DOE cannot entirely rely on systems left over from the Cold War. For a long time, DOE's security controls have emphasized "guns, guards, and gates," as well as strict control over anyone, including foreign visitors, allowed to enter the weapons laboratories. Where visitors went, whom they talked to, and what they saw were more carefully controlled than they are today. These controls, while still necessary in some places, cannot be expected to work in locations where openness, collaboration, and free access to information and ideas are encouraged. In these places, DOE needs a more sophisticated security strategy that is consistent with the laboratories' more open missions and includes a greater role played by DOE and laboratory counterintelligence programs.

Now more than ever, effective counterintelligence efforts must be central to DOE's security strategy. Greater counterintelligence program effectiveness can be achieved through the development of a comprehensive threat assessment to determine the nature, extent, and targets of foreign espionage efforts against DOE's weapons laboratories. Such an assessment could also form the basis for developing counterintelligence program performance measures as well as periodic headquarters evaluations of each laboratory's performance. These evaluations would determine how effectively each laboratory is addressing the established performance measures and how their counterintelligence programs can be improved.

In addition to establishing performance measures for DOE's counterintelligence program, other parts of the overall strategy could be improved by clarifying what constitute sensitive subjects, tightening procedures for background checks, and reassessing procedures for foreign visits to controlled areas. For example, clarifying what subjects are

sensitive and requiring an independent review by technically qualified personnel of all subjects proposed for discussion during a visit would help ensure that researchers, program managers, and DOE headquarters officials would have the same understanding of what needs to be protected so discussions of sensitive subjects would not occur without the knowledge of DOE. DOE and laboratory officials recognize the problems with identifying sensitive subjects and have established internal review processes to better focus on those foreign visits that involve sensitive subjects. However, without a clear understanding of what information DOE considers sensitive, these improved review processes cannot provide adequate assurance that foreign visits involving sensitive subjects are appropriately identified and reviewed.

Increasing the number of background checks on foreign visitors from sensitive countries will enable DOE to better assess individual situations from a security point of view. When necessary, actions can then be taken to mitigate the risks of a particular visit. While background checks cannot identify all foreign visitors who pose a risk, they are a valuable tool for alerting DOE and the laboratories of situations that may warrant more attention and control. DOE's current foreign visitor order contains requirements that would increase the number of background checks obtained; enforcing those requirements at the laboratories, especially at Los Alamos and Sandia, should enable DOE to expand its advance knowledge of risks associated with the visits and, if necessary, mitigate those risks.

Finally, a specific assessment of vulnerabilities related access to unclassified, but sensitive information in controlled areas is needed. This assessment will help ensure that procedures for these areas are consistent from laboratory to laboratory and security vulnerabilities and/or problems are identified and corrected. In addition, this assessment could identify best practices that DOE could disseminate for use to all laboratories for improving the protection of sensitive information that may be exposed to foreign visitors.

Recommendations

We recommend that the Secretary of Energy:

- Direct DOE's Counterintelligence Division to perform a comprehensive assessment of the espionage threat against DOE and the weapons laboratories to serve as the basis for determining appropriate countermeasures and resource levels for laboratory counterintelligence

programs. To the extent possible, this assessment should include the laboratories as well as other agencies with appropriate expertise, such as the FBI and CIA.

- Establish appropriate program performance measures and expectations for the laboratories' counterintelligence activities and require periodic performance reviews to help determine if their activities are effectively preventing foreign espionage.
- Revise DOE's foreign visitor order to (1) clarify to all DOE and laboratory contractor personnel the specific types of unclassified, but sensitive, subjects that require protection from compromise by foreign nationals and (2) require that the subjects of visits be independently reviewed by experts with appropriate technical backgrounds—such as laboratory individuals involved in export control issues—to verify that visits involving sensitive subjects are adequately identified for DOE's review.
- Require that DOE and the weapons laboratories comply with the current foreign visitor order by obtaining background checks on all assignees from sensitive countries. Further, require the laboratories to inform headquarters of the names of all other proposed foreign visitors from sensitive countries so DOE's Counterintelligence Division can obtain additional background checks at its discretion.
- Require that security measures at each laboratory's controlled areas—those most accessible to foreign visitors—be assessed to ensure that the controls over persons and information in these areas are effective. This assessment should also identify the best practices at each laboratory to improve protection of sensitive information that may be exposed to foreign visitors.

DOE's Comments and Our Response

DOE had no comments on the general nature of the facts in the report and concurred with our recommendations. The Department, however, believes that the report overstates the value of background checks on foreign visitors. DOE believes that foreign intelligence services increasingly rely on "non-official collectors"—who would have clear background checks—instead of intelligence officers. We do not believe we are overvaluing background checks. We recognize that these checks are but one factor DOE considers in approving foreign visits. Nevertheless, the information obtained through background checks can be of importance in determining if additional risk is associated with a foreign visitor. Consequently, we are recommending that DOE complete background checks in accordance with its foreign visits and assignments order.

DOE also suggested that we revise our recommendation on the assessments of information security in controlled areas. A key point in DOE's suggested revision was to have the recommendation specify that an operations security assessment be done of each laboratory's controlled areas, whereas we recommended only that an assessment be done. We did not revise our recommendation to specify this type of assessment because, while we believe that operations security principles and personnel must be part of any assessment of the laboratories' controlled areas, other elements of DOE's security programs can also provide value in an assessment. We do not want to be overly prescriptive on how and/or by whom these assessments be done. DOE also suggested that the wording of the recommendation more clearly focus on protecting sensitive information. We revised the recommendation to clarify that the assessments should identify the best practices to improve the protection of sensitive information. Finally, DOE's response detailed a number of actions it has taken or plans to take to address the recommendations. We did not address these actions as part of our work. The full text of DOE's comments are included in appendix IV.

DOE's List of Sensitive Countries

Algeria
Armenia
Azerbaijan
Belarus
China
Cuba
Georgia (Republic of)
India
Iran
Iraq
Israel
Kazakhstan
Kyrgyzstan
Libya
Moldova
North Korea
Pakistan
Russia
Sudan
Syria
Taiwan
Tajikistan
Turkmenistan
Ukraine
Uzbekistan

DOE's List of Sensitive Subjects

DOE 1240.2B
8-21-92

Attachment 5
Page 1

SENSITIVE SUBJECTS

This is a list of areas of technical subject matter or technologies that are considered to be "sensitive." The list identifies subjects related to nuclear weapons and the prevention of the proliferation of nuclear weapons and also identifies other sensitive technologies.

Topics Related to Nuclear Weapons and Nonproliferation*

1. Nuclear weapons production and supporting technologies.
2. Nuclear explosion detection and evaluation.
3. Production, handling and metallurgy of thorium, uranium, and plutonium.
4. Uranium enrichment. Discussions regarding contractual and related program matters concerned with the provision of U.S. uranium enrichment services and other non-U.S. marketing activities conducted under the purview of the Assistant Secretary for Nuclear Energy are not considered "sensitive" subjects as defined in this Order.
5. Large-scale tritium production technology.
6. Lithium isotope production.
7. Heavy water production.
8. Uranium hexafluoride production.
9. Fuel fabrication.
10. Reprocessing technology. "(Civilian program not considered sensitive in respect to a country with which DOE has an international agreement or contract.)"
11. Physical security systems and procedures related to protection of nuclear and other sensitive facilities.
12. Production of reactor-grade zirconium, graphite and beryllium.
13. Advanced nuclear reactor systems, space and mobile reactors, naval nuclear reactors. (The Assistant Secretary for Nuclear Energy requires that approval authorities at field locations ensure prior consultation with the Office of Nuclear Energy before approving any visits or assignments involving its programs in these subject areas). Light water, gas-cooled, and liquid metal cooled reactors are not considered to be "sensitive" unless one of the topics in items 9 through 12 above are involved.
14. Inertial confinement fusion.

*More detailed descriptions of the items in this list can be found in the Nuclear Technology Reference Book.

Appendix II
DOE's List of Sensitive Subjects

Attachment 5
Page 2

DOE 1240.2B
8-21-92

Other Sensitive Subjects*

Certain additional unclassified subjects are considered to be "sensitive" if they fall into one or more of the following categories:

1. Technologies or aspects of the technology that are under export control, i.e., equipment, services to that equipment, or technical data related to that equipment that require review and approval before export;
2. Technologies or certain aspects of the technology that are "dual-use," i.e., those technologies that have a peaceful application and also have a militarily critical application and are proposed for export control; or
3. Technologies that are advancing rapidly such that a reasonable projection of the militarily critical applications of the technology would cause certain aspects of the technology to become classified or placed under export control.

Specific technologies qualifying as "Other Sensitive Subjects" are listed below:

Computer systems and computer component development, specifically designed for military application.
Computer security procedures involving encryption.
Secure computer-controlled communications systems.
Computer software specifically designed for military applications.
Advanced concepts of computer-aided design, computer-aided manufacturing, and computer-aided testing.
Manufacturing and fabrication techniques for high performance materials.
Directed energy systems technologies, including:
extremely high energy, high brightness lasers;
extremely high current, high brightness particle beams;
high kinetic energy macro particle accelerators;
very high power radio frequency power sources, involving very short or very long wavelengths; and
high energy electrical power conditioning systems for these technologies.
Techniques for preparation of ultra-high purity semiconductor materials.
Very high speed instrumentation and diagnostics, as may be applicable to directed energy systems and weapons development.
High energy density batteries and fuel cells.
Fabrication techniques for very high field, large bore superconducting magnets.

*More detailed descriptions of the items in this list can be found in the Militarily Critical Technologies List.

Number and Percentage of Background Checks Obtained for Foreign Visitors From Sensitive Countries to DOE's Nuclear Weapons Laboratories, 1994-96

Country ^a	Livermore			Los Alamos			Sandia		
	Visits	Checks	Percent	Visits	Checks	Percent	Visits	Checks	Percent
Algeria	8	7	88	6	0	0	2	0	0
Armenia	1	0	0	6	0	0	1	0	0
Azerbaijan	0	1	^b	1	0	0	0	0	•
Belarus	12	7	58	13	0	0	15	0	0
China	474	185	39	746	12	2	244	2	1
Cuba	4	1	25	0	0	•	0	0	•
Georgia (Republic of)	0	0	•	0	0	•	4	0	0
India	193	85	44	407	5	1	214	7	3
Iran	26	11	42	20	0	0	19	0	0
Iraq	2	1	50	3	0	0	4	0	0
Israel	60	27	45	114	0	0	58	2	3
Kazakhstan	8	2	25	37	0	0	15	2	13
Kyrgyzstan	0	0	•	1	0	0	0	0	•
Libya	2	0	0	0	0	•	0	0	•
Moldova	0	0	•	3	0	0	0	0	•
Pakistan	6	2	33	8	1	13	16	0	0
Russia	653	302	46	1,110	116	10	474	33	7
Syria	2	3	^b	5	0	0	0	0	•
Taiwan	65	33	51	97	3	3	43	1	2
Turkmenistan	0	0	•	0	0	•	7	0	0
Ukraine	47	22	47	69	0	0	38	1	3
Uzbekistan	0	1	^b	0	0	•	2	0	0

^aThe following countries that changed status from sensitive to nonsensitive during 1994 are not included in this table: Argentina, Brazil, Bulgaria, Burma, Cambodia, Chile, El Salvador, Ethiopia, Romania, South Africa, South Korea, Vietnam, and Yugoslavia.

^bAccording to DOE, background checks outnumbered visits for Azerbaijan, Syria, and Uzbekistan because checks may have been obtained for planned visits that were later canceled.

Source: GAO's analysis of data from DOE and the weapons laboratories.

Comments From the Department of Energy



Department of Energy
Washington, DC 20585

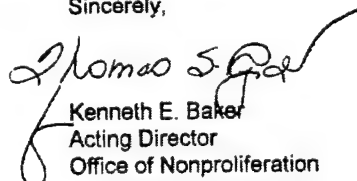
September 17, 1997

Mr. Victor S. Rezendes
Director
Energy, Resources
and Science Issues
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Rezendes:

The Department of Energy appreciates the opportunity to review the draft General Accounting Office report, "Department of Energy: Actions Needed to Improve Controls Over Foreign Visitors to Weapons Laboratories." We have no comments on the general nature of the facts as they are portrayed. However, we have attached our comments on the recommendations cited in the report.

Sincerely,


Kenneth E. Baker
Acting Director
Office of Nonproliferation
and National Security

Attachment

Comments on
Draft General Accounting Office Report
"Department of Energy: Actions Needed to Improve Controls
Over Foreign Visitors to Weapons Laboratories"
RCED-97-229, August 28, 1997

Recommendation 1

Direct DOE's counterintelligence office to perform a comprehensive assessment of the espionage threat against DOE and the weapons laboratories to serve as the basis for determining appropriate countermeasures and resource levels for laboratory counterintelligence programs. Such an assessment should, to the extent possible, include the laboratories and other agencies with expertise, such as the FBI and CIA.

Management position

Concur.

To assess the espionage threat against the Department, the Counterintelligence Division has implemented measures to bridge the gap between the counterintelligence and the foreign intelligence elements in the weapons laboratories. It has added a strategic analysis capability in order to integrate the counterintelligence and foreign intelligence functions throughout the complex. In this manner, the Department will develop a new understanding of how to attack the problem while institutionalizing a process that couples strategic and tactical analysis. This will serve as a basis for determining countermeasures and resource levels for laboratory counterintelligence programs. Specifically, a career foreign intelligence analyst was added to the counterintelligence division and given responsibility for the counterintelligence program funds devoted to analysis. Additionally, the laboratories are developing various threat assessment methodologies to provide a framework for a comprehensive analysis of the threat. Finally, these measures will tie together efforts by the Department's complex with the knowledge base of the Intelligence Community to produce an overarching assessment of the threat facing the Department.

Recommendation 2

Establish appropriate program performance measures for the laboratory's counterintelligence activities and require periodic performance reviews to help determine if their activities are effectively preventing foreign espionage.

Management position

Concur.

This is a major concern of the Department. The Department's Counterintelligence Program Order mandates that the Counterintelligence Division develop standards, provide oversight, and ensure compliance for departmental counterintelligence activities, but does not itself set performance standards. The "Counterintelligence Procedural Guide" likewise establishes process but articulates no performance standards. Based on these authorities, however, the division is now establishing specific performance standards for laboratory counterintelligence programs. General qualitative standards are being established for the program, and quantitative standards will follow in specific topical areas. An example of this is the "Counterintelligence Debriefing Program Handbook" published in August 1997. This document clearly establishes the program's purpose, objectives, and scope. It further states the Headquarters' responsibility for program evaluation, both overall and at each location. The handbook mandates that each site institute quality assurance processes and details the primary, secondary, and tertiary priorities of the program, i.e., which travelers and hosts of foreign visitors should receive the greatest attention. The Department's laboratories will direct their counterintelligence resources using these priorities. The handbook also describes expectations regarding subject coverage, documentation, etc. Quantitative guidelines will be established jointly with each site, pending assessment of experience with these qualitative standards. This process will serve as a model for other portions of the counterintelligence program. Work is also under way on establishing a feedback mechanism, either site specific or program wide, so that problem areas need not await formal evaluation to be addressed. The Department agrees that periodic performance reviews will determine whether these standards are being met. Past efforts were hampered by the lack of established performance standards. Criteria were usually inferred from the procedural guide and there was not always agreement on interpretation. Moreover, results of the assessments were non-binding and were without enforcement of counterintelligence program standards at the laboratories. Additionally, some counterintelligence positions in the laboratories are now funded directly by Headquarters, which will afford increased leverage in compliance matters.

Recommendation 3

Revise the foreign visitor order to (1) clarify to all DOE and laboratory contractor personnel the specific types of unclassified, but sensitive subjects that require protection from compromise by foreign nationals and (2) require that the subjects of visits be reviewed by independent parties with appropriate technical backgrounds—such as laboratory individuals involved in export control issues—to verify that visits involving sensitive subjects are adequately identified for DOE review.

Management Position

Concur.

The Department agrees with the General Accounting Office on the urgency of this issue. During November 1996, then Deputy Secretary Curtis made the issue of "what the Department should strive to protect" a priority to investigate.

The Department is reviewing the current visits and assignments program and will change, modify, and/or implement the following: (1) the current visits and assignments database is undergoing minor modification to improve user interface until such time as a new database system becomes operational; (2) a new visits and assignments database system will be developed using the Internet as a communications backbone, a netscape-type of customer interface and input device, and a modern relational database on a network server; and (3) the Department's Order on unclassified visits and assignments will be revised and published. During this review of the Order, the Department's program managers will determine whether the goal of the order is to protect sensitive subjects or be aware of individuals from sensitive countries, or a hybrid of both. The overall point is one of clarifying the sensitive subjects that require protection from compromise, and applying the knowledge to actual foreign national visits and assignments.

Should the Sensitive Subjects List be reviewed and updated, this guidance will be provided to appropriate individuals at all departmental sites. This will be led by the Department's Nuclear Transfer and Supplier Policy Division, which last updated the Sensitive Subject List in 1994 at the request of the visits and assignments management community. Any technical specifications that are presented in a revised list will have to remain at the unclassified level. Realizing that the General Accounting Office has recommended that the Department present detailed specifications in each subject category so that explicit guidance is available to the laboratories, in many cases, this guidance would have to be classified. The Department will attempt to help the visits and assignments management community to focus on clarification of how to use the sensitive subject list. Requiring an independent quality assurance check on the identification of sensitive subjects will assist in the Department's efforts to improve controls on foreign visitor access. The identification of one individual at each site responsible for determining whether a visit involved a sensitive subject would increase the effectiveness of guidance from the visits and assignments management community regarding the use and interpretation of the Sensitive Subject List.

The Department also believes that any determination of a subject's sensitivity, and associated measures to protect it, must be based on a process. The Department's counterintelligence perspective believes a sensitive country visitor or assignee poses a collection risk no matter where they go in the laboratory, and technology should not be the final determinant in authorizing foreign national presence at the

laboratories. As with the visits and assignments management community, there needs to be greater participation by the laboratories scientists, independent reviewers, and collaboration with the Intelligence Community in deciding what to protect and to what degree. As an example, the Lawrence Livermore National Laboratory has made great strides in this direction. They have brought together all the appropriate parties, such as export control and security and counterintelligence, to finalize risk management policy about individual foreign national visits. The balance will shift from the previous default position *that foreign access was approved, unless there were clamorous objections*, to one where *foreign access will be tightly scrutinized, taking into account such factors as current status of the technology, the foreign national's country or program of origin, need for access, and the potential for loss or damage to US interests.*

Recommendation 4

Require that DOE and the laboratories comply with the current foreign visitor order by obtaining background checks on all assignees from sensitive countries. Further, require the laboratories to inform headquarters of the names of all other proposed foreign visitors from sensitive countries so DOE's Counterintelligence Division can obtain additional background checks at its discretion.

Management position

Concur.

The Department agrees in general that indices or records checks are an important information source on prospective foreign visitors/assignees. However, the Department believes the report overstates the value of indices checks as a counterintelligence risk determinant. Based on what we know about the foreign intelligence collection, we believe there is little likelihood that foreign intelligence services would resort to aggressive, high-risk collection techniques (e.g., stealing documents, surreptitious photography, cold pitching (contacting) laboratory personnel) when less intrusive means are available. This means that foreign intelligence services increasingly rely on non-official collectors, scientists, academics and arms control inspectors, for example, instead of intelligence officers to do the collection. Usually these individuals have had no affiliation with intelligence and security services; hence, there is little likelihood of a positive indices check. This leads to another problem inherent in our use of indices checks—false negatives.¹

¹ This issue was addressed at length in a June 1990 study entitled, "The Intelligence Threat to US Government Facilities From Visiting Foreign Nationals: An Intelligence Community Assessment."

When there is a "no record" or "no derogatory" response, there is a natural tendency to assume a visitor/assignee is not a collector and therefore not a security risk. Often just the opposite is true. Even when indices checks are positive, the information is often dated or ambiguous or irrelevant. While we continue to support the value of indices checks, we cannot use them as a litmus test for risk assessment.

There are other effective ways to deal with the potential of foreign collection at the labs. One is to expand the briefing/debriefing program, making it mandatory that all Department and laboratory personnel having contact with sensitive country nationals, either through visits/assignments or reciprocal visits to sensitive countries, must be briefed/debriefed by the Department's counterintelligence officers. As we have expanded our counterintelligence debriefing program over the past year, there has been a significant increase in counterintelligence incident reporting. This information is entered into a database and becomes available to counterintelligence offices across the departmental complex. Over time, as the database expands, the counterintelligence database may surpass (but not replace) indices checks as an analytical tool. Beyond their purely substantive contribution, the indices process provides the Department's counterintelligence professionals with a much needed entree into the foreign visits and assignments process.

Recommendation 5

Require that an assessment of each laboratory's controlled areas--those most accessible to foreign visitors--be conducted to ensure that the controls over persons and information in these areas is adequate. This assessment should examine and identify the best practices at each laboratory to improve DOE's foreign visitor controls.

Management Position

Concur.

The Department agrees with the spirit of the recommendation; however, we suggest the General Accounting Office change the language of the recommendation to capture the intended message better. Rather than "... an assessment of each laboratory's controlled areas--those most accessible . . .," the Department recommends the following: "Require the Department to conduct an Operational Security (OPSEC) assessment of each laboratory's controlled areas--that are susceptible to access by foreign visitors--to ensure the adequacy of information and physical security controls. These assessments should examine and identify the best practices at each laboratory to improve protection of classified and sensitive unclassified information that may be exposed to the Department's foreign visitors."

The purpose of this change is to help the Department ensure that all areas subject to foreign visitor access, and not just "... most accessible to ...," are reviewed for adequacy of information controls. We substituted language regarding the controls of foreign visitors with wording concerning protection practices of classified and sensitive unclassified information. Controls placed on the foreign visitors are but one portion in the overall information protection effort and should be incorporated as an element in appropriate security plans.

The Department's Headquarters element, in concert with respective Operations Offices and Laboratories, will conduct an OPSEC assessment of each of the laboratory's controlled areas. Additionally, the Department will consider removing all exemptions and exceptions to policy, based on location, area or brevity of visit, concerning foreign national tracking, monitoring and control. The objective is not to "improve protection" for a single area, but to say with 100% assurance that foreign nationals are never inadvertently exposed to classified information, and that sensitive technologies are only accessed by foreign nationals after a clear determination that US interests warrant such disclosure, on a case-by-case basis.

Major Contributors to This Report

Resources,
Community, and
Economic
Development Division
Washington, D.C.

Gary L. Jones, Associate Director
William F. Fenzel, Assistant Director
Dave Brack
John R. Schulze

Denver Regional
Office

James C. Charlifue
Frank B. Waterous